

APPLICATION FOR UNITED STATES LETTERS PATENT

for

**SYSTEM FOR OBTAINING SIGNATURES ON A SINGLE AUTHORITATIVE COPY
OF AN ELECTRONIC RECORD**

by

Charles F. Hawkins, Donald James Plaster, and Scott G. Ainsworth

Peter A. Shaddock, II
Patent Attorney
Kaufman & Canoles
One Commercial Place, Suite 2000
Norfolk, VA 23514
(757) 624-3169

Seto Patents
617 Tinkerbelle Rd.
Chapel Hill, N.C. 27514
(919) 960-8836

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to the field of computer security, especially relating to electronic records.

2. Description of Related Art

Modern technology has profoundly changed the way business transactions are conducted today. The use of computers and other data processing devices are now commonplace in both large and small businesses. The connectivity provided by intranets and the Internet have reduced information transfer times from days down to seconds. For a reasonable investment, small businesses and even non-profit organizations can acquire communications benefits similar to those of large high-technology corporations.

Governments, too, have taken advantage of the cost and time savings benefits offered by electronic communications. Electronic filing of U.S. income tax returns is now the preferred method of filing a return by the U.S. government. Transferring documents electronically eliminates postage and shipping charges and allows documents to be received at their destination almost instantaneously.

In recognition of the general acceptance of using electronic communications in the business place, laws regulating electronic communications have begun to be developed and adopted. More laws are likely to come about, or existing laws revised, as acceptance of electronic communications continues to grow and become more highly developed in the future.

The purpose of laws, such as the Uniform Electronic Transactions Act (UETA) and the e-Sign Act, is to validate the authority of electronic transactions to legally bind one party to another party, and to provide a legal framework for enforcement.

The system described in this patent application is a system for secure, enforceable electronic communications.

An understanding of several industry-standard definitions is necessary to be able to evaluate the importance of this system and compare it with other solutions

30 currently available or that may become available as the use of electronic business transactions continues to increase.

An *electronic transaction* is any type of business that is conducted by electronic means, such as by computer, Personal Device Assistants (PDAs), and other devices not yet invented. For example, the transaction may consist of ordering
35 a book or other product from a Web site and making payment by electronic means, such as providing credit card information or debiting the payment from a checking account.

An *electronic record*, according to the Electronic Signatures in Global and National Commerce Act (E-Sign), is "a contract or other record created, generated,
40 sent, communicated, received, or stored by electronic means."¹ The E-Sign Act further states that a record must be retrievable in perceivable form.²

A *repository* is the secure environment in which electronic records are maintained. The repository must encompass sufficient security methods to ensure safe storage and integrity of the electronic record.

45 An *electronic signature* is "an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."³

A *message digest* is a compressed representation of an electronic record. Message digests are produced using standard, published, one-way hashing
50 algorithms. Message digests produced by the same algorithm generally are the same length in bits. The message digest will be considered a unique valid representation of the electronic record because it is computationally infeasible for two different electronic records to produce the same message digest while using the same message digest function.

55 Message digest algorithms currently on the market, such as MD-2, MD-4, MD-5, SHA-1, and SHA-256, take specific portions of the record (512 bits or 1024 bits) and create a message digest of that portion. This hash of the set length of bits

¹ Electronic Signatures in Global and National Commerce Act (E-Sign), Sec. 106 (4).

² Ibid. Sec. 106 (9).

³ Ibid. Sec. 106 (5).

produces a set of hex chain values. The chain values are summed bitwise along with a seed value to produce the final message digest. For SHA-1, as an example, five 32-bit chain values are produced for each 512 bits of data. A full history of Public Key Cryptography (PKC) systems is described in W. Diffie's, "The First Ten Years of Public-Key Cryptography," which is incorporated herein by reference.

A digital signature is a form of electronic signature, generated by computer hardware or software and represented in a computer as a string of binary digits. The methods of producing a digital signature involve a set of rules and a set of parameters such that the digital signature produced is unique and verifiable. Both the identity of the signatory (person represented by the digital signature) and the integrity of the data (binary bits making up the digital signature) can be verified. Today, the first step in generating a digital signature is typically the generation of a message digest, usually much smaller than the electronic record on which it is based. The message digest will be unique because it is computationally infeasible for two different electronic methods to produce the same message digest on the same electronic record; therefore, the use of a message digest as a representation of the electronic record is considered valid. The second step in generating a digital signature is to cryptographically combine the message digest and an asymmetric private key. Standards for generation of digital signatures will be known to those of ordinary skill in the art.

A Public Key Cryptography (PKC) system is an asymmetric encryption system, meaning that it employs two keys, one for encryption and one for decryption or validation of what is encrypted. Asymmetric systems adhere to the principle that knowledge of one key (the public key) does not permit derivation of the second key (the private key). Thus, PKC permits the user's public key to be posted, in a directory or on a bulletin board for example, without compromising the user's private key. This public key concept simplifies the key distribution process. Popular PKC systems make use of the fact that finding large prime numbers is computationally easy but factoring the products of two large prime numbers is computationally

infeasible. Example PKC algorithms are the Digital Signature Algorithm (DSA)⁴, the Rivest, Shamir, and Adleman (RSA) algorithm, as specified in Internet Engineering Task Force (IETF) Request for Comments (RFC) 2347 and its successors.

90 A *private key* is the half of a Public Key Cryptography (PKC) pair that is kept private and secret, and is used to generate a digital signature.

 A *public key* is the half of a PKC pair that is published, and is used to verify a digital signature. Each person involved in an electronic transaction based on the private and public key method of digital signature generation and verification will
95 possess a private and public key pair. A public key may be known to the public in general, but a private key is never shared. Anyone can verify a person's digital signature by using that person's public key, but only the possessor of a person's private key may generate a digital signature. More information about how public keys and private keys work is contained later in this section.

 Typically, public and private keys are used as the means of allowing for the generation and verification of digital signatures. Public-key encryption schemes, commonly called PKC, are well known and utilize a public key and a private key that are mathematically related. Based on a public-key/private-key pair, digital messages can be encrypted by either of the keys and decrypted by the other, with the public
100 keys recorded in a public directory, which is publicly accessible, and the private key privately retained. Typically, the signer of the message accesses the public-key directory and retrieves the receiver's public key. Then the signer encrypts the message with the receiver's public key, and conveys the encrypted message to the receiver. The receiver, upon receiving the encrypted message, decrypts the
105 message with his private key.
110

 PKC can also be used to generate a digital signature to authenticate the signer. Typically, the signer creates a message digest of the electronic record. After generating the message digest, the signer creates a digital signature from the message digest with his private key. The receiver, upon receiving the digital

⁴ Federal Information Processing Standards Publication 186 (1994) ("FIPS PUB 186," and its successors).

signature and the message, uses the signer's public key to verify the signature. This process is performed iteratively until the entire electronic record has been hashed. This operation ensures the identity of the signer because he is the only person who can encrypt the message with his private key.

Besides the PKC method, another encryption method is the symmetric algorithm. An example of this is the Data Encryption Standard (DES), which is described in Data Encryption Standard, Federal Information Processing Standards Publication 46 (1977) ("FIPS PUB 46," and its successors) that are available from the U.S. Department of Commerce. In general, a symmetric cryptographic system is a set of instructions, implemented in either hardware, software, or both, that can convert plain text into ciphertext, and vice versa. In a symmetric cryptographic system, a specific key is used that is known to the users but is kept secret from others.

A blue ink signature is a physically-produced signature made by a person using an ink pen, regardless of the color of the ink or the legibility of the signature. An "X" or a scribble can suffice as a legally-binding signature provided that both parties involved in the transaction have agreed upon the existence of an ink mark in a particular area or areas of the physical record constitutes agreement by the signer to the terms contained within the physical record. When the agreement states that a witness or notary public must observe and verify that the signer did intend to demonstrate agreement to the terms of the physical record by placing an ink signature, or mark, in the appropriate areas, then the signature and/or stamp of a witness or notary public must be present on the physical record in order for the transaction to be legal and enforceable.

A person is defined as "an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity."⁵

An authoritative copy is the best available copy of a document. The best available document may indeed be the original, but when an exact original cannot be

⁵ Electronic Signatures in Global and National Commerce Act (E-Sign), Sec. 106 (8).

found, then the best available copy of a document becomes the authoritative copy.

145 The authoritative copy must be clearly identifiable as an authoritative copy. Thus, the authoritative copy must be associated with a means of establishing, identifying, maintaining, and enforcing control of the authoritative copy.

150 Current law has established that senders and receivers of transferable electronic records have rights equal to those of senders and receivers of equivalent paper records.

155 The significance of current acts such as the Electronic Signatures in Global and National Commerce Act (E-Sign) and the Uniform Electronic Transactions Act (UETA) is that electronic records, exchanged between two parties who have agreed to conduct a transaction by electronic means, and with the ability for the electronic records to be retrieved by both parties, shall be valid, legal transactions enforceable just as if they contained "blue ink" signatures. "Retrieved," as used in the preceding sentence, means the document must be able to be stored and printed by the receiver.

160 Computers and other electronic devices, such as Personal Digital Assistants (PDA) and cellular telephones, provide the interface terminals from which parties to a business transaction may take advantage of the many benefits of electronic communications. One of the most important benefits of electronic communications is the ability to communicate and transact business with a person, or groups of people, almost anywhere in the world. Electronic communications can take place over 165 telephone lines, the Internet, and through the air via cellular and satellite communication systems.

170 Computers, and other electronic devices, receive digital information into their memory and present the information to a user. The information can be present in different ways, such as visual displays, voice and other audio output through a speaker, and by printing the information. A combination of the output methods, commonly referred to as multimedia, is intended to enhance the user's understanding of the communicated information. Computers and other electronic devices can display information in the form of text, graphs, pictures, and video.

175 It should be understood that for purposes of this patent application, we are
defining an electronic transaction environment as any technology that allows two
computers to communicate with each other. Thus, the words electronic and digital
are essentially interchangeable. A network, intranet, or The Internet is not necessary;
for example, a PDA could communicate with a standalone computer using infrared
signalling. The process of retrieving files from one computer or interface terminal
180 device (such as a PDA) to another is called downloading. The process of sending
files to another computer or interface terminal is called uploading.

Computers and hardware alone are not sufficient to complete electronic
transactions. Software is also needed to provide for security between the
transacting parties and to allow the parties to digitally sign electronic records.

SUMMARY OF THE INVENTION

185 The invention sets forth a secure method of processing and/or handling of
electronic records. In the Background of the Invention section, we presented an
overview and definitions related to electronic records. In this section, we address
currently known problems associated with electronic transactions, and describe how
190 our invention resolves these problems.

A key problem associated with electronic records is the potential to have
many duplicates. The invention allows and guarantees a unique copy of an
electronic record.

195 A secure and legally enforceable electronic transaction must allow for the
secure maintenance of control of the resulting electronic record. For the purposes of
this patent application, *repository* is the term used to describe the secure
environment in which the electronic record is maintained.

200 The electronic record in the repository is referred to as the authoritative
electronic record. Control is maintained in the repository by software and at least
one secure computer. The authoritative electronic record may represent a legally
enforceable writing. A copy of the authoritative electronic record can be
electronically transmitted over a network to a computer. This copy of the

authoritative electronic record can be used to digitally sign the authoritative
electronic record, which remains at the repository.

The copy of the authoritative record can be viewed, printed, and saved at, as
well as retransmitted from, the remote location without compromising the integrity of
the authoritative record at the repository. The method comprises receiving an
electronic record in the repository, creating an authoritative electronic record of the
received record by appending information to the end of the electronic record, digitally
signing the electronic record and appended information to form a receipt, prepending
this receipt information to the beginning of the electronic record, appending
additional information to the end of the electronic record, and storing this whole as
the authoritative electronic record in the repository. The authoritative electronic
record is unique since no other representation of it exists anywhere else. The
concatenated whole of all information prepended to the beginning of the record is
referred to as the *beginning information*. The concatenated whole of all information
appended to the end of the electronic record is referred to as the *ending information*.

When a copy of the authoritative electronic record is requested by a person at
a remote location, a copy is made by making a copy of the electronic record and the
appended ending information only. The system then provides for transmitting a
version of the copy to the person at the remote location, wherein transmission may
be over the un-trusted network, and the copy of the authoritative electronic record
may be printed and stored at the remote location. Software at the remote location
provides for receiving the version of the copy of the authoritative electronic record
and digitally signing the authoritative electronic record. A message digest is created
by combining a partial message digest from the repository with the remaining
message digest information from the copy of the authoritative electronic record and
identifying information of the new digital signature, at the remote location. The digital
signature on the authoritative electronic record at the repository is then created at
the remote location using this message digest just created at the remote location and
the private key. The person then transmits the new digital signature and identifying
information of the new digital signature back to the secure environment where the

repository provides for validating the digital signature of the authoritative electronic
record signed at the remote location against the existing authoritative electronic
record stored at the repository through standard digital signature validation
techniques.

Upon affirmative validation of the digital signature, a revised authoritative
electronic record is generated. The revised authoritative electronic record is created
by prepending the digital signature to the existing beginning information of the
authoritative electronic record, appending additional information to the ending
information of the authoritative electronic record, and storing the revised authoritative
electronic record in the repository. The additional information appended to the
ending information can include information indicating authorization for generating the
revised authoritative electronic record, signatory information, and other information.

A key point of the present invention is that it leaves only one copy of a unique
authoritative electronic record. The present invention does not prevent the ability to
make copies of the record, but it does ensure that copies made are easily
distinguished as copies.

Another key point of the present invention is that it allows a person to
electronically sign an electronic record at a remote location without compromising
the uniqueness of a corresponding authoritative electronic record.

Another key point of the present invention is to provide a method for revising
authoritative electronic records that is secure, verifiable, and includes clear
identification of involved parties.

The method our system uses meets all of the above requirements.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention of the present application will now be described in more detail
with reference to the accompanying drawings, given only by way of example, in
which:

Figure 1 is a block diagram of communication links between the present
apparatus and remote locations;

Figure 2 is a block diagram showing receipt of a record at a repository,
generation of an authoritative record in the repository, and the transmission of a copy
of the authoritative record to a remote location;

Figure 3 is a block diagram showing the generation of a digital signature at a
remote location and the transmission of that digital signature to the repository;

Figure 4 is a block diagram showing generation of a revised authoritative
record, copying of the revised authoritative record, and transmission of the copy to a
remote location;

Figure 5 is a flow chart illustrating the overall operation of the present system;

Figure 6A is a flow chart illustrating the receipt of a record in the secure
environment;

Figure 6B is a flow chart illustrating the steps involved in making a copy of an
authoritative record;

Figure 6C is a flow chart showing the generation of a digital signature by a
person at a remote location and its validation at the repository;

Figure 6D is a flow chart showing the steps of generating a revised
authoritative record at the repository.

DETAILED DESCRIPTION OF THE INVENTION

Figure 1 shows remotely located computers 1-3 connected to the present
repository 5 via a network 4. Computers 1-3 represent all electronic devices that can
transmit and display a record, such as other servers, personal computers, laptop
computers, personal digital assistants (PDAs), and cellular telephones. Network 4
includes the Internet and other networks, such as private local area networks
(LANs), over which the electronic record may be transmitted. Repository 5
comprises one or more secure servers and record maintenance software for
ensuring the integrity of electronic records therein. Of course a computer or other
electronic device may also be directly connected to repository 5.

Figure 2 shows the initial operation of the present system. Record 6 is sent
from a remote location to the repository 5. Record 6 is receipted within repository 5

by prepending receipt 7 to the beginning of record 6 and appending receipt 8 to the
end of record 6. In an exemplary embodiment, receipt 7 is the repository's digital
signature of record 6 and identifying information. Receipt 8 is an un-encrypted
message digest of record 6 and the identifying information. Identifying information
can include a time-stamp and the originator of the record. All information that has
been encrypted, including actual digital signatures in Figures 2-4, is shown in
double-framed format.

In operation, a time-stamp is attached to every record received in the present
repository. The time-stamp includes time and date of receipt in the repository. The
receipted record 6-8 is now the authoritative record or authoritative copy of the
record and is stored in a secure location within the repository 5. The concatenated
whole of all information prepended to the beginning of the record 6 is referred to as
the beginning information. The concatenated whole of all information appended to
the end of the record 6 is referred to as the ending information.

When a person at a remote location requests the authoritative record, to
review or to sign, record maintenance software stored and executed in repository 5
produces a distinct copy of the authoritative record. All copies that are made of an
authoritative record, in this system, comprise the record and the record's ending
information. Receipt 7, the only beginning information in our example so far, is
notably missing from the copy 6 and 8 that is sent to the requesting person. In this
embodiment, the copy 6 and 8 is encrypted 9 with a shared secret symmetric key
while being transmitted to the remote location. At the remote location, the person
decrypts the encrypted copy 9 using the shared secret symmetric key. The person is
then able to view, store, and print the copy.

Figure 3 begins with the process of signing the authoritative record at the
remote location. The person at the remote location has in their possession the copy
of the authoritative record 6 and 8. In order to sign the authoritative record 6-8, the
person first needs to compute a message digest of the authoritative record 6-8.
However, since the remote location does not have receipt 7, the person cannot
immediately compute the required message digest. Sending an exact copy of

receipt 7 to the remote location would destroy the uniqueness of the authoritative record 6-8 stored in the repository 5. In order to maintain the uniqueness of authoritative records in the repository 5, only a representation of the beginning information, receipt 7 in this case, is sent to the remote location. A partial message digest 10 is computed at the repository 5 that is based on all of the beginning information. In this case, the partial message digest 10 is only based on receipt 7. The partial message digest 10 is composed of at least two pieces of information, the interim chaining values (defined below) and the digital length in bits of the prepended beginning information.

The interim chaining values are computed in two steps. The first step involves padding to a known bit value the existing beginning information with the necessary bits to make the bit length of the beginning information an integer multiple of the bit length in each message digest algorithm. The same message digest algorithm will also be employed to complete the message digest used in the desired digital signature at the remote location. The second step involves inputting the now padded bit stream of the beginning information into the message digest algorithm to produce the interim chaining values. This process of creating the chaining values is called "interim" because the final hashing of the entire message is not completed at the repository 5. Rather, this final hashing will be completed at the remote location.

Once the partial message digest 10 is computed in repository 5, the resulting partial message digest 10 must be transmitted to the remote location. The person at the remote location receives partial message digest 10 and uses the partial message digest 10 to reseed the same message digest algorithm mentioned above and finishes generating a complete message digest by inputting his copy 6 and 8. The complete message digest represents copy 6 and 8 and receipt 7. Optionally, additional identifying information from the remote location may be included with identifying information 8 when the message digest is computed.

The person then uses his private key to create a digital signature with the complete message digest, thereby signing the receipted record 6-8 and producing digital signature 11. The digital signature 11 may include encoding information. In

355 this embodiment, a small hardware token or smart card provides the private key used by the person for encryption. Alternatively, in some circumstances, a software-based private key may be used. Digital signature 11 along with any identifying information is then transmitted to repository 5 where it is validated with the public key and a recomputed message digest of receipted record 6-8. A positive match validates the digital signature 11 and establishes that:

- 360 (1) the record 6 and ending information in the repository 5 are the same as the record 6 and ending information communicated to the remote location;
- (2) the signer had the private key necessary to digitally sign the authoritative record;
- 365 (3) a digital signature has been obtained for the authoritative record and any additional identifying information provided for digital signature 11;
- (4) the process of transmitting the record 6, ending information 8, and partial message digest 10 from the repository 5 to the remote location where the message digest was completed was successful;
- 370 (5) the process used to compute the digital signature was performed correctly by the electronic device at the remote location; and,
- (6) the process of transmitting the digital signature 11 and any identifying information from the remote location to the repository 5 was successful.

Continuing in Figure 3, after validation of the digital signature 11, the process of revising the authoritative record begins by prepending digital signature 11 to the beginning of the authoritative record 6-8, and appending signature information 12 to the end of authoritative record 6-8. In this embodiment, signature information 12 comprises any identifying information included in the message digest for the digital signature, the message digest used to produce the digital signature, and a timestamp. Of course, more or less information can be included or excluded from the signature information 12. The operation of revising the authoritative record is continued in Figure 4.

375

380

Referring to Figure 4, digital signature 11 has been prepended to, and signature information 12 has been appended to, the authoritative record 6-8, thus

increasing the amount of beginning and ending information, respectively. The repository 5 can then receipt the signed record 6-8 and 11-12, by prepending a repository-created digitally signed receipt 13 to, and appending identifying receipt information 14 to, the signed record. The receipted signed record 6-8 and 11-14 is now the "revised authoritative record" replacing the earlier authoritative record 6-8. When further requests are received for a copy of the record, the revised authoritative record 6-8 and 11-14 will be used to generate the copies following the procedure outlined in the discussion of Figure 2. As shown in Figure 4, the copy of the revised authoritative record will consist of record 6 and all ending information; appended information 8, 12, and 14, in this case. The process of transmitting a copy of the authoritative record over the partially un-trusted network 4 is then repeated, wherein the transmission is normally encrypted with a symmetric key to produce encrypted copy 15 which the requestor decrypts using the symmetric key at a remote location.

Figure 5 is a flow chart for the overall operation of the present system. In step S500, an electronic record is sent to the repository 5 from a remote location. In step S502, a unique authoritative record is created and stored within repository 5. When a person at a remote location wants to sign the authoritative record, a copy of the authoritative record is made that is distinctly different from, but perceptively the same as, the authoritative record. The distinctly different copy and a partial message digest for the beginning information are sent to the person, at step S504. The copy of the authoritative record and the partial message digest can, of course, be sent in two separate steps. In step S506, the message digest is completed at the remote location using the copy of the authoritative record as input, and the remote location uses a private key and the completed message digest to create the digital signature. The digital signature is then transmitted to the repository 5 where it is validated and upon affirmative validation, the authoritative record is revised with the digital signature, step S508.

Figures 6A-6D provide a detailed flow chart of exemplary embodiments for carrying out the method discussed in association with Figure 5. In Figure 6A, an exemplary embodiment for receipting a record in repository 5 and generating the

initial authoritative record is illustrated. In step S600 the record is received in the present repository, which may also be referred to as a trusted repository. In step S602 a time stamp, which may include other identifying information, is completed for and appended to the record. The phrase "receipted record" refers to any record received by the secure environment that has been time-stamped. Step S604 is the first step in generating the initial authoritative record.

The authoritative record is important because the authoritative record is the record that must remain unique, to ensure legal enforceability under current electronic transaction laws. In step S604, a message digest is generated of the record and time stamp. In step S606 the message digest is digitally signed to create a receipt, and the receipt is then prepended to the beginning of the record. The prepended receipt and any later prepended information is referred to as "beginning information". In step S608 identifying information related to the receipt is appended to the end of the record. The appended identifying information identifies the receipt as the repository's signature and includes other information. The appended information and any later appended information is referred to as "ending information". The record together with beginning information and ending information make up the "authoritative record" and at step S610 the authoritative record is stored in the repository 5.

Figure 6B is a flow chart detailing an exemplary method of transmitting a distinct copy of the authoritative record. In step S612, a request is received from a remote location for a copy of an authoritative record in the repository 5. In step S614, the copy is made by copying only the record and ending information of the requested authoritative record. The copy of the authoritative record is then transmitted, in an industry-standard encrypted manner, over a network that may be partially un-trusted, in step S616. It may be noted at this point that a copy of an authoritative record is now in the hands of a person at a remote location, but the authoritative record in the repository is still unique. At step S618, the requestor is free to store and print the copy of the authoritative record at the remote location for thorough review prior to signing.

Figure 6C details the signing operation by a person at a remote location.

445 Prior to signing the authoritative record, portions of the record maintenance software have been loaded on the signatory's computer or workstation. At step S620 the person decides to sign the authoritative record. In order to sign the record the person must first create a message digest of the authoritative record. Since the person at the remote location does not have the beginning information, which was
450 retained in the repository 5, the software requests additional information from the repository 5. At step S622, the repository 5 in response generates a partial message digest using the beginning information as input and transmits the partial message digest to the remote location. The partial message digest comprises interim chaining values of the beginning information and the length of the beginning information. If by
455 chance a second person has signed the same authoritative record, between the time the first person requested the record at step S612 and decided to sign the record at step S620, then the system takes appropriate steps to make sure the first person receives and signs a revised authoritative record. Primarily, the first person is notified of the new signature and is sent a revised copy and a revised partial message digest. The person then continues with the normal signing process
460 described below.

At step S624 the person receives the partial message digest. At step S626, the remote location uses the interim chaining values of the partial message digest to reseed the message digest algorithm and complete a message digest for the
465 authoritative record that was begun in the repository 5. In step S628 the resulting message digest, and any user added information, is then digitally signed with the person's private key, thereby generating a digital signature. In step S630 the digital signature is transmitted to the repository 5. And in step S632 the signature is validated in the repository 5. The first step in validation is computing a message
470 digest of the authoritative record stored in the repository 5 and any additional identifying information added by the signer on his copy of the message digest.

Using this authoritative record message digest, the uploaded digital signature, and the corresponding public key, the digital signature is validated by either using a

validating algorithm in the case of a DSA-type digital signature or message digest
comparison in the case of a RSA-type digital signature. A validation or perfect match
indicates a valid digital signature.

Figure 6D illustrates the steps for revising the authoritative record once a
digital signature has been validated. A decision is made in step S634. If the digital
signature was not validated in step S632 then the process must restart at step S614
where a new copy will be made and sent to the remote location. If, at step S634, the
signature was determined to be valid, then we proceed to step S638 where
authorization is given to create a revised authoritative record. Generating a revised
authoritative record, in a preferred embodiment, involves prepending the digital
signature to the beginning of the current authoritative record and appending
signature information to the end of the current authoritative record. In step S640 the
digital signature is prepended to the beginning of the authoritative record. It should
be understood that the digital signature may have additional information attached
thereto prior to prepending. In step S642 signature information, which includes the
message digest used to create the digital signature at the remote location, is
appended to the end of the authoritative record. In step S644 a receipt of the
partially revised authoritative record is prepended to the beginning of the partially
revised authoritative record, i.e., the beginning of the prepended digital signature.
And in step S646 identifying information for the receipt of the partially revised
authoritative record is appended to the end of the partially revised authoritative
record, i.e., to the end of the signature information. This combination of the digital
signature and repository receipt prepended to the "old" authoritative record and the
signatory information and identifying information appended to the "old" authoritative
record is the "revised authoritative record". At step S648 the revised authoritative
record is stored in a repository 5. It should also be understood that previous artifact
records, receipts, digital signatures, and identifying information may also be
maintained separately in the repository 5.

The foregoing description of the specific embodiments will so fully reveal the
general nature of the invention that others can, by applying current knowledge,

readily modify and/or adapt for various applications such specific embodiments
505 without departing from the generic concept. For example, a revised authoritative
record could be created with only one beginning information and one ending
information appended to the prior authoritative record. Therefore, such adaptations
and modifications should and are intended to be comprehended within the meaning
and range of equivalents of the disclosed embodiments. It is to be understood that
510 the phraseology of terminology employed herein is for the purpose of description and
not of limitation.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225